What is claimed is:

1. A method, comprising:

identifying a user using unique information;

designating a first plurality of files in a computer as being associated with said user;

responsive to said identifying, using a program to allow said user to make a change to any of said first plurality of files associated with said user; and

preventing reading contents of said first plurality of read/write files when said user is not identified.

2. A method as in claim 1, wherein said preventing comprises encrypting said files using an encryption value which requires said unique information to form an encryption key.

3. A method as in claim 2,wherein said specified information includes a user password.

4. A method as in claim 2,wherein said specified information includes a unique number indicative of hardware in the computer system.

5. A method as in claim 1, further comprising designating a second plurality of files on the computer as read only, and storing unencrypted information in said read only files, but not allowing any changes to said read only files.

6. A method as in claim 5, further comprising establishing a plurality of special files within said plurality of files, said special files being unencrypted read/write files, and establishing special security measures for said special files.

7. A method as in claim 6, wherein said security measures include determining whether a specified program is actually accessing the file, and only allowing file access by said specified program.

8. A method as in claim 1,further comprising detecting certain kinds of accesses based on specified security criteria, and maintaining a log of said accesses including information about a program that made said accesses.

9. A method as in claim 1, wherein said preventing comprises preventing certain users from obtaining access to said files.

10. A method, comprising:

storing both encrypted and unencrypted files on a computer;

starting an operating system by reading said unencrypted files, and storing encrypted information indicating results of computer operations.

11. A method as in claim 10, further comprising designating unencrypted files as read only, and encrypted files as read/write files.

12. A method as in claim 10, further comprising forming encrypted files by requiring a unique information, and using said unique as part of an encryption and/or decryption operation.

13. A method as in claim 11, further comprising establishing special files which are read/write files that are not encrypted, and carrying out at least one security measure on said special files.

14. A computer, comprising:

a processor;

a file accessing element, controlled by a controlling operation, said file accessing part controlling files in the computer in a way that prevents access to specified files but allows access to other files unless specific unique information is used.

15. A computer as in claim 14, wherein said file accessing element allows access to all read only files, and prevents access to read/write files without said unique information.

16. A computer as in claim 15, wherein said file accessing element allows access to certain read write files which are designated as being special, and also conducts a security check before allowing said access to said read write files.

17. A computer as in claim 14, wherein said file accessing part controls said access by encrypting said files.

18. A computer as in claim 17, wherein said encrypting comprises obtaining personal information from a user, and using said personal information to form encryption and/or decryption operations.

19. A computer as in claim 18, wherein said personal information is a password.

20. A computer as in claim 14, further comprising a file storage part which includes removable memory, and wherein unencrypted read/write access is allowed to said removable memory.

21. A computer as in claim 14, wherein said file accessing element is part of an operating system.

22. A method comprising:

identifying a user using unique information;

using an operating system associated program of a computer to designate a first plurality of files in a computer, as being associated with said user and to encrypt said plurality of files using an encryption system that includes said unique information;

responsive to said identifying, using said operating system associated program in said computer to allow said user to make any changes to any of said first plurality of files using said encryption system associated with said user and to prevent reading contents of said first plurality of read/write files when said user is not identified;

allowing other unencrypted files on said system to be read when said user is not identified, but preventing writing to said other unencrypted files; and

establishing special files on said system which are unencrypted but which can be written to and read by the system only after a specified security operation.

23. A method, comprising:

obtaining a unique code from a user of the computer system;

determining specified files on the computer system which qualify for a specified security aspect; and

encrypting all other files other then said specified files on said computer system, using said unique code.

24. A method as in claim 23, wherein said unique code is a password.

25. A method as in claim 23, wherein said unique code is a code from a smart card.

26. A method as in claim 23, wherein said unique code is a code from a biometric.

27. A method as in claim 23, wherein said unique code is a code from a digital certificate.